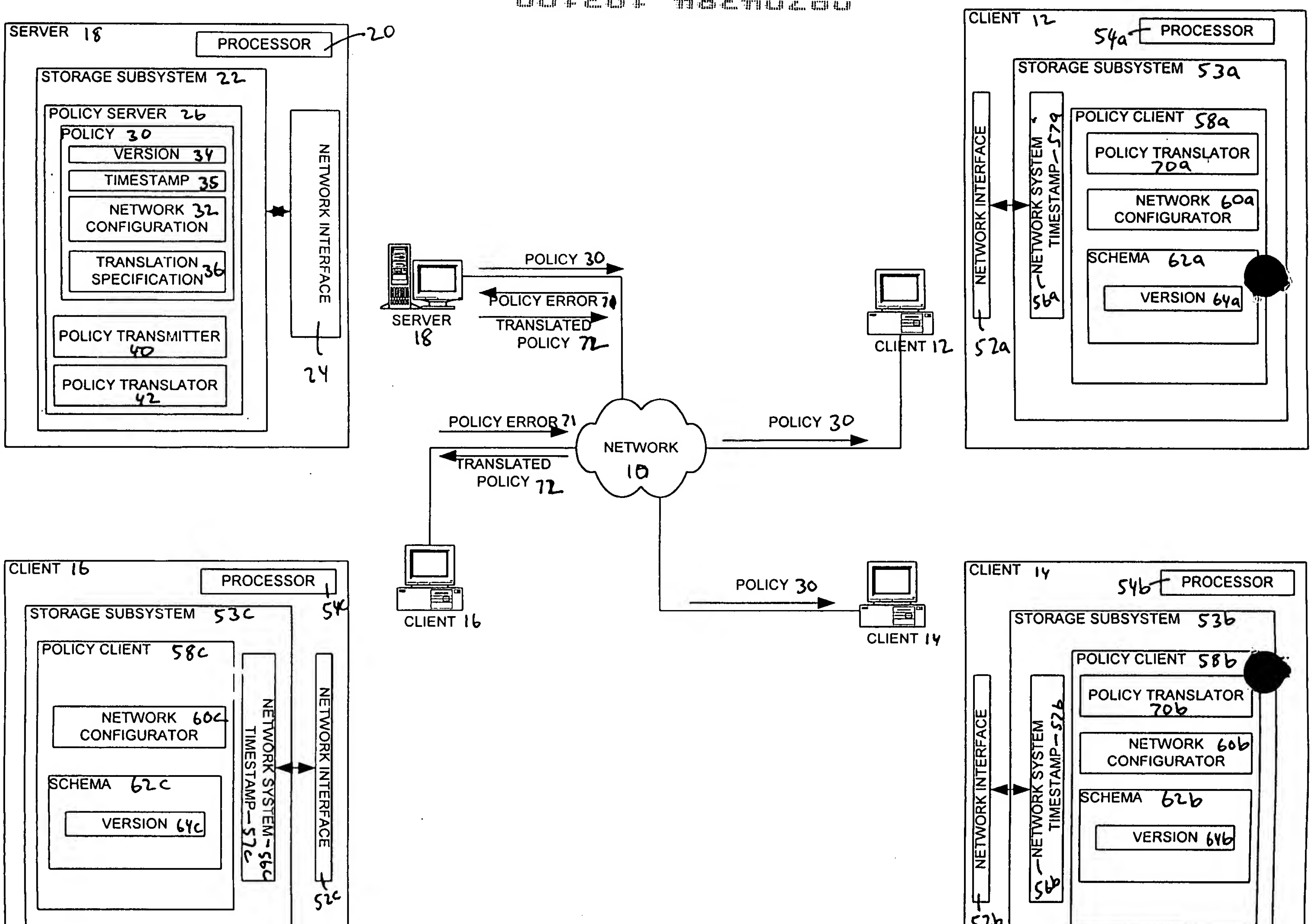
SERVER 18
PROCESSOR
20
STORAGE SUBSYSTEM 22
POLICY SERVER 26
POLICY 30
VERSION 34
TIMESTAMP 35
NETWORK 32
CONFIGURATION
TRANSLATION
SPECIFICATION 36
POLICY TRANSMITTER
40
POLICY TRANSLATOR
42
NETWORK INTERFACE
24
SERVER
18
POLICY 30
POLICY ERROR 71
TRANSLATED
POLICY 72
POLICY ERROR 71
TRANSLATED
POLICY 72
NETWORK
10
POLICY 30
POLICY 30
CLIENT 12
CLIENT 14
CLIENT 16
CLIENT 12
54a
PROCESSOR
STORAGE SUBSYSTEM 53a
NETWORK INTERFACE
52a
NETWORK SYSTEM
TIMESTAMP—57a
56a
POLICY CLIENT 58a
POLICY TRANSLATOR
70a
NETWORK 60a
CONFIGURATOR
SCHEMA 62a
VERSION 64a
CLIENT 16
PROCESSOR
54c
STORAGE SUBSYSTEM 53c
POLICY CLIENT 58c
NETWORK 60c
CONFIGURATOR
SCHEMA 62c
VERSION 64c
NETWORK SYSTEM—56c
TIMESTAMP—57c
NETWORK INTERFACE
52c
CLIENT 14
54b
PROCESSOR
STORAGE SUBSYSTEM 53b
POLICY CLIENT 58b
POLICY TRANSLATOR
70b
NETWORK 60b
CONFIGURATOR
SCHEMA 62b
VERSION 64b
NETWORK INTERFACE
52b
NETWORK SYSTEM
TIMESTAMP—57b
56b

Fig. 1

```
// Policy that conforms to the newer schema (specifies Rjindael):

<?xml version="1.0"?>

<!DOCTYPE IPsecPolicyOnSystem PUBLIC "//somestandard.org/IPsecPolicy/Version1.1">

<IPsecPolicyOnSystem timestamp="2000-9-30_12:12:12">

        <IKEProposals>

            <IKEProposal id="Proposal1" CipherAlgorithm="DES" HashAlgorithm="MD5" GroupId="DH768" AuthenticationMethod="Preshared"/>

            <IKEProposal id="Proposal2" CipherAlgorithm="Rjindael" HashAlgorithm="SHA-1"    GroupId="DH1024" AuthenticationMethod="DSS_Signatures"/>

        </IKEProposals>

</IPsecPolicyOnSystem>
```

Fig. 2

```
// DTD schema Version 1.1 for IPsec implementations that support the new
// encryption algorithm called Rjindael:

<?xml version="1.0" encoding="UTF-16"?>

<!ELEMENT IKEProposal EMPTY>

<!ATTLIST IKEProposal
    id ID #REQUIRED
    CipherAlgorithm (3DES | DES | IDEA | Blowfish | RC5 | CAST | Rjindael) #REQUIRED
    HashAlgorithm (MD5 | SHA-1 | Tiger) #REQUIRED
    GroupId (DH768 | DH1024 | DH1536 | ECC2N155 | ECC2N185) #REQUIRED
    AuthenticationMethod (DSS_Signatures | Preshared | RSA_Signatures |
    RSA_Encryption | Revised_RSA_Encryption | Kerberos) #REQUIRED
>

<!ELEMENT IKEProposals (IKEProposal+)>

<!ELEMENT IPsecPolicyOnSystem (IKEProposals)>

<!ATTLIST IpsecPolicyOnSystem
        timestamp CDATA #REQUIRED
>
```

Fig. 3

```
// DTD schema for version 1.0 IPsec policy implementations (doesn't
// include the new encryption algorithm called Rjindael):

<?xml version="1.0" encoding="UTF-16"?>

<!ELEMENT IKEProposal EMPTY>

<!ATTLIST IKEProposal

        id ID #REQUIRED

        CipherAlgorithm (3DES | DES | IDEA | Blowfish | RC5 | CAST) #REQUIRED

        HashAlgorithm (MD5 | SHA-1 | Tiger) #REQUIRED

        GroupId (DH768 | DH1024 | DH1536 | ECC2N155 | ECC2N185) #REQUIRED

        AuthenticationMethod (DSS_Signatures | Preshared | RSA_Signatures |

        RSA_Encryption | Revised_RSA_Encryption | Kerberos) #REQUIRED

>

<!ELEMENT IKEProposals (IKEProposal+)>

<!ELEMENT IPsecPolicyOnSystem (IKEProposals)>

<!ATTLIST IPsecPolicyOnSystem

        timestamp CDATA #REQUIRED

>
```

132

131

130

Fig. 4

```
// XSLT file to transform the above policy into a policy conforming to the older
// schema. This transformation simply replaces attribute "Rjindael" with "3DES".

<?xml version="1.0" encoding="UTF-8"?>
<!-- This stylesheet replaces the CipherAlgorithm Rjindael with 3DES, for IKE
implementations that do not support Rjindael. -->
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
    <xsl:output method="xml" version="1.0" encoding="UTF-8" indent="yes"/>

    <xsl:output doctype-public="//somestandard.org/IPsecPolicy/Version1.0"/>   146

        <xsl:template match="/*">
    <xsl:element name="IPsecPolicyOnSystem">
    <xsl:copy-of select="@*"/>
    <xsl:element name="IKEProposals">
    <xsl:apply-templates select="IKEProposals"/>
    </xsl:element>
    </xsl:element>
    </xsl:template>

    <xsl:template match="IKEProposals/IKEProposal">

        <xsl:element name="IKEProposal">
            <xsl:copy-of select="@*"/>

            <xsl:if  test="@CipherAlgorithm = 'Rjindael'">   142a
   142
                <xsl:attribute name="CipherAlgorithm">3DES</xsl:attribute>   142b

            </xsl:if>

        </xsl:element>

    </xsl:template>

</xsl:stylesheet>
                                                  36
```

Fig. 5A

```
// Output resulting from applying the above transformation to the policy:

<?xml version="1.0" encoding="utf-8"?>

<!DOCTYPE IPsecPolicyOnSystem PUBLIC "//somestandard.org/IPsecPolicy/Version1.0">

<IPsecPolicyOnSystem timestamp="2000-9-30_12:12:12">

<IKEProposals>

        <IKEProposal id="Proposal1" CipherAlgorithm="DES" HashAlgorithm="MD5" GroupId="DH768" AuthenticationMethod="Preshared"/>

        <IKEProposal id="Proposal2" CipherAlgorithm="3DES" HashAlgorithm="SHA-1" GroupId="DH1024" AuthenticationMethod="DSS_Signatures"/>

</IKEProposals>

</IPsecPolicyOnSystem>
```

Fig. 5B

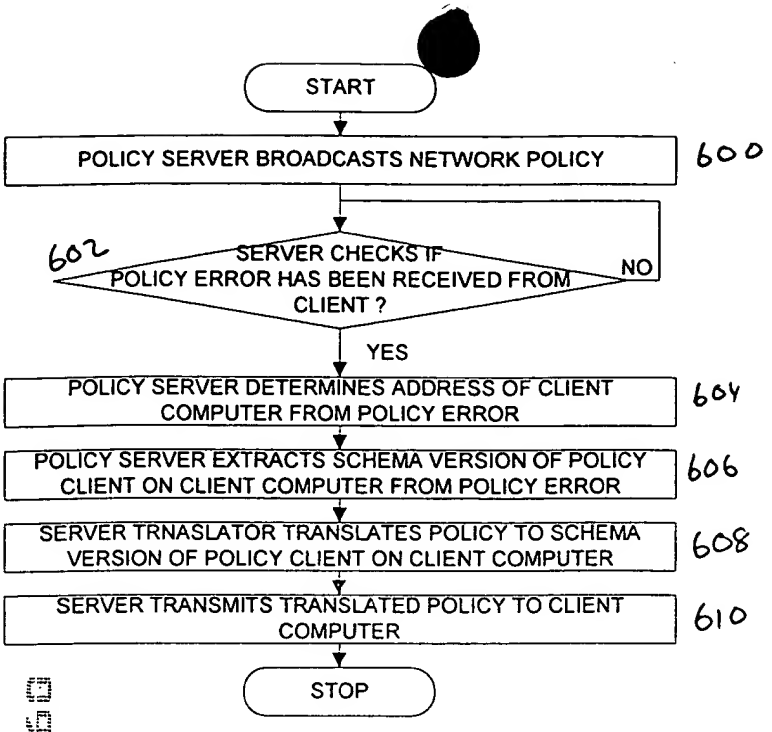
START
POLICY SERVER BROADCASTS NETWORK POLICY
600
602
SERVER CHECKS IF POLICY ERROR HAS BEEN RECEIVED FROM CLIENT ?
NO
YES
604
POLICY SERVER DETERMINES ADDRESS OF CLIENT COMPUTER FROM POLICY ERROR
604
POLICY SERVER EXTRACTS SCHEMA VERSION OF POLICY CLIENT ON CLIENT COMPUTER FROM POLICY ERROR
606
SERVER TRNASLATOR TRANSLATES POLICY TO SCHEMA VERSION OF POLICY CLIENT ON CLIENT COMPUTER
608
SERVER TRANSMITS TRANSLATED POLICY TO CLIENT COMPUTER
610
STOP

FIG. 6

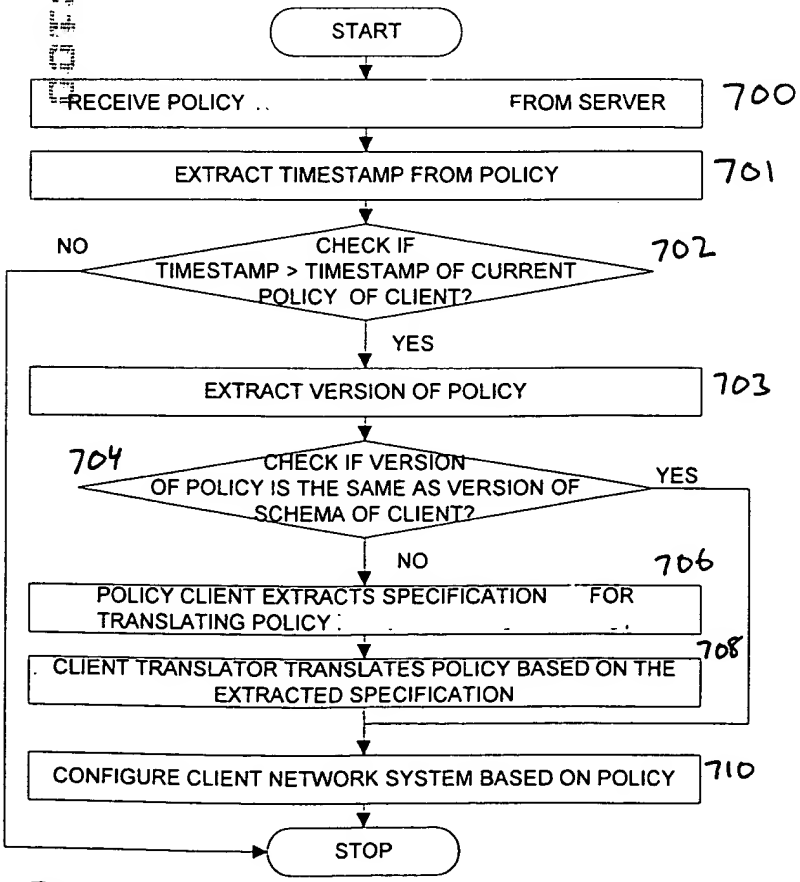
START
RECEIVE POLICY .. FROM SERVER
700
EXTRACT TIMESTAMP FROM POLICY
701
NO
CHECK IF TIMESTAMP > TIMESTAMP OF CURRENT POLICY OF CLIENT?
702
YES
EXTRACT VERSION OF POLICY
703
704
CHECK IF VERSION OF POLICY IS THE SAME AS VERSION OF SCHEMA OF CLIENT?
YES
NO
706
POLICY CLIENT EXTRACTS SPECIFICATION FOR TRANSLATING POLICY
CLIENT TRANSLATOR TRANSLATES POLICY BASED ON THE EXTRACTED SPECIFICATION
708
CONFIGURE CLIENT NETWORK SYSTEM BASED ON POLICY
710
STOP

FIG. 7A

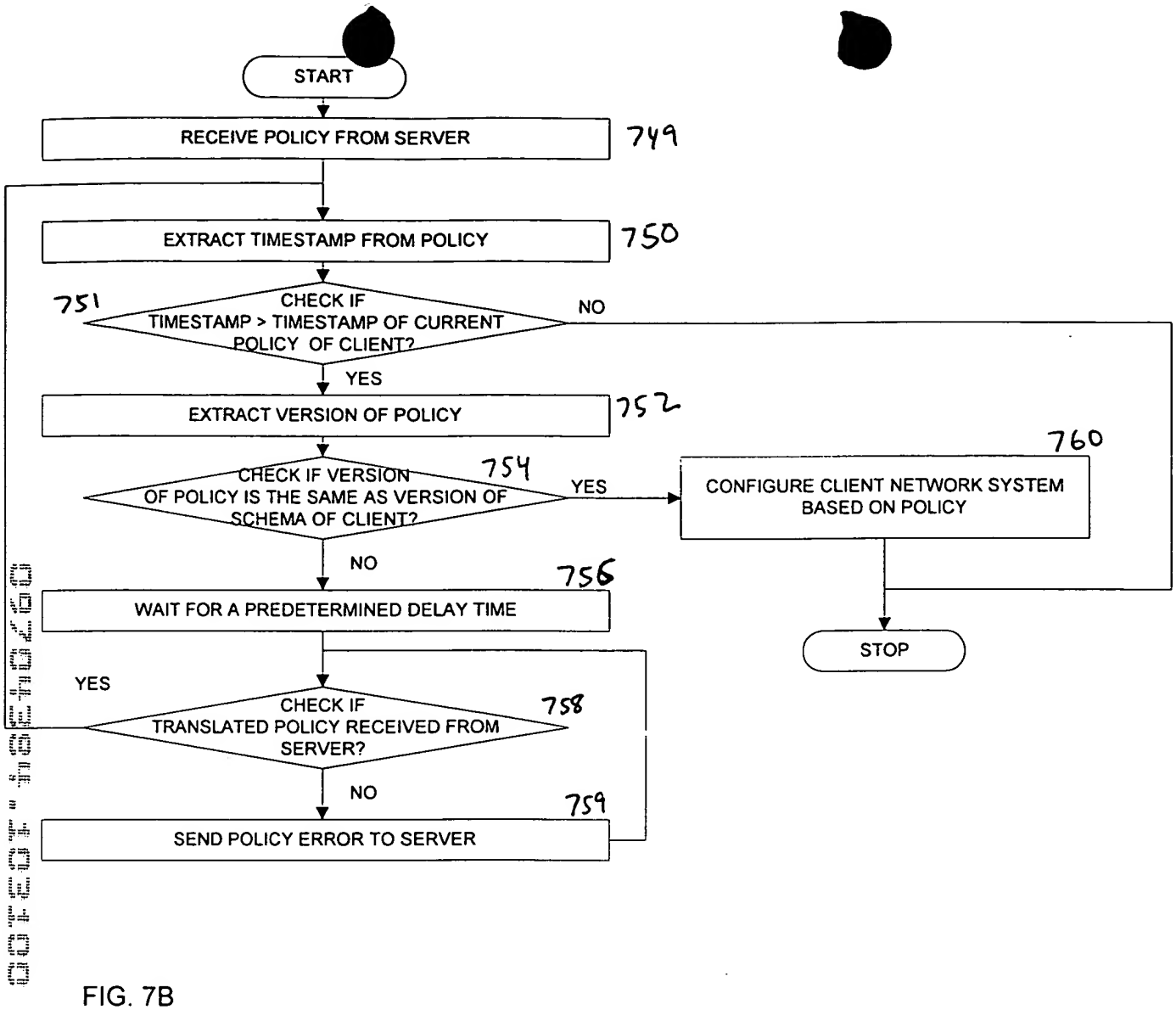
START
RECEIVE POLICY FROM SERVER
749
EXTRACT TIMESTAMP FROM POLICY
750
751
CHECK IF TIMESTAMP > TIMESTAMP OF CURRENT POLICY OF CLIENT?
NO
YES
EXTRACT VERSION OF POLICY
752
760
754
CHECK IF VERSION OF POLICY IS THE SAME AS VERSION OF SCHEMA OF CLIENT?
YES
CONFIGURE CLIENT NETWORK SYSTEM BASED ON POLICY
NO
756
WAIT FOR A PREDETERMINED DELAY TIME
STOP
YES
758
CHECK IF TRANSLATED POLICY RECEIVED FROM SERVER?
NO
759
SEND POLICY ERROR TO SERVER

FIG. 7B